UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

2012 COMMERCIAL ST SE, APT A, ALBUQUERQUE, NEW MEXICO 87102

Case No. **25mr934**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-2, which is attached hereto and incorporated herein.

located in the _____ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 846	Conspiracy to Distribute Controlled Substances
18 U.S.C. §§ 371 and 1791	Conspiracy to Attempt to Provide a Prohibited Object to an Inmate of a Prison.

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

_____
Applicant's signature

Deputy United States Marshal Tyler K Foster
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephonically sworn and electronically signed *(specify reliable electronic means)*.

Date: May 20, 2025

_____
Judge's signature

City and state: Albuquerque, New Mexico

The Hon. Laura Fashing, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF: 1812 DEL NORTE DRIVE SW, ALBUQUERQUE, NM 87123; AND 2012 COMMERCIAL ST SE, APT A, ALBUQUERQUE, NEW MEXICO 87102	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

1. I, Tyler K Foster, Deputy United States Marshal ("DUSM") of the United States Marshal Service ("USMS"), being first duly sworn, make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the following premises (collectively, the "Subject Premises"):

A-1: 1812 Del Norte Drive SW, Albuquerque, New Mexico 87105; and

A-2: 2012 Commercial St SE Apt A, Albuquerque, New Mexico 87102.

2. More detailed descriptions and photographs of the Subject Premises are contained within Attachments A-1 and A-2, which have been attached hereto and incorporated herein by this reference.

PURPOSE OF THE AFFIDAVIT

3. The USMS and the Federal Bureau of Investigation ("FBI") Albuquerque Division Violent Gang Task Force ("VGTF") have been engaged in an investigation of several gang members and drug traffickers involved in drug distribution within the Cibola County Correctional

Center[1] ("CCCC") located in Milan, New Mexico. The investigation pertains to an intergang conspiracy between CCCC inmates, gang members who are not incarcerated, and their criminal associates, to distribute controlled substances within CCCC.

4. This affidavit is submitted in support of a warrant to search the Subject Premises, which is believed to contain evidence of conspiracies to commit drug distribution and the introduction of contraband into a federal jail facility. This affidavit supports a search for evidence of violations of the below violations, collectively referred to hereinafter as the "Target Offenses":

a. 21 U.S.C. § 846: Conspiracy to Distribute Controlled Substances; and

b. 18 U.S.C. §§ 371 and 1791: Conspiracy to Provide a Prohibited Object to an Inmate of a Prison.

5. I am submitting this affidavit based upon my experience and familiarity with the instant investigation. This affidavit does not set forth all of my knowledge or summarize all of the investigative efforts in the overall investigation; rather, this affidavit sets forth facts that support probable cause to search the requested locations and persons, as well as relevant background information.

6. I make this affidavit based upon my own personal knowledge, which is substantially derived from my participation in the investigation, as well as that of fellow agents and officers who have participated in the investigation. In addition, I have developed information I believe to be reliable from additional sources including:

a. Information provided by Task Force Officers ("TFO"), Special Agents

[1] Cibola County Correctional Center is controlled and operated by CoreCivic, which is a private company that provides corrections, detention, and reentry services to local, state, and federal government.

("SA"), and Intelligence Research Specialists ("IRS") of the FBI and USMS, and other law enforcement officials ("agents"), including oral and written reports that I have received directly or indirectly from said investigators;

b. Results of physical surveillance conducted by agents during the investigation;

c. Information derived from consensually recorded conversations and video surveillance footage;

d. A review of driver's license and automobile registration records; and

e. Records from the National Crime Information Center ("NCIC").

7. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

AFFIANT'S RELEVANT TRAINING AND EXPERIENCE

8. I am a Deputy United States Marshal with the USMS and have been since July 19, 2022. I have received and completed training at the Federal Law Enforcement Training Academy ("FLETC") as a criminal investigator. During my tenure with the USMS, I have investigated and assisted in the apprehension of federal, state, and local fugitives to include but not limited to sex offenders, gang members, violent repeat offenders, and those with extensive criminal history.

9. In conjunction with my current assignments as a member of the USMS Southwest Investigative Fugitive Team ("SWIFT"), I am assisting the FBI VGTF with the ongoing criminal investigation into drug distribution and the introduction of contraband into CCCC.

10. Through my work with the USMS and VGTF, I have become familiar with matters including, but not limited to, the means and methods used by individuals to purchase, transport, store, and distribute drugs and to hide profits generated from those transactions. I am particularly familiar with the techniques traffickers use to smuggle drugs into CCCC.

EVIDENCE SOUGHT DURING SEARCH

11. Based on my training, experience and participation in this and in similar investigations, I believe that individuals involved in illegal trafficking of controlled substances into CCCC often conceal evidence of their illicit income in their residences, and in surrounding areas to which they have ready access such as garages, carports and outbuildings. They also conceal evidence in vehicles, including vehicles outside of their residences and businesses, so that they have ready access to it and so that they can hide it from law enforcement, including law enforcement officers executing search warrants at their residences. This evidence can be found in the form of U.S. currency, or banking and investment account statements. These records can be maintained on paper, but also can be maintained as electronic data on computers and other digital media.

12. Based on my training, experience and participation in this and in similar investigations, I believe that individuals involved in illegal trafficking of drugs and contraband into CCCC may maintain documents referencing specific inmates, as well as communications with those inmates or other complicit guards working within CCCC. For example, a correctional officer may maintain a ledger showing money owed for contraband delivered, or notes with an address and scheduled time to pick up a package for subsequent smuggling into the facility.

13. Individuals involved in this smuggling may also keep controlled substances, such as methamphetamine and suboxone, in their residences and vehicles. These individuals have to pick controlled substances up from drug trafficking organizations and transport them to CCCC, and may split larger shipments into smaller packages to make them easy to conceal, including in clothing, or secret in their body cavities.

14. Individuals involved in smuggling contraband into CCCC use firearms as tools of the trade. The substances that these individuals plan to smuggle are valuable, and they cannot call the police if their controlled substances are stolen. They thus keep firearms in close proximity to themselves, and their product and proceeds, to protect them from thieves and law enforcement.

15. Individuals involved in smuggling contraband and controlled substances into CCCC are likely to have extensive contact with co-conspirators via mobile phones, laptops, or other communication devices. The collection of contraband and consolidation of inmate funds are not tasks that one complicit guard can generally accomplish on his or her own—they require coordination between co-conspirators. And given that the remoteness of CCCC from large-scale DTOs in Albuquerque, much of this communication does not occur face-to-face. This communication can occur in the form of phone calls, text messages, SMS (Short Message Service) messaging, MMS (Multimedia Messaging Service) messaging, social media posts and messaging, and smartphone application messaging services. Smartphones, tablets, cellular phones, and digital devices are frequently capable of storing messages, emails, social media communications, and communications made over smartphone applications. The content of these communications will often provide evidence of smuggling.

16. Many individuals involved in these activities take photographs and videos of the contraband, or the proceeds from smuggling it, either to prove to co-conspirators that they are fulfilling their part or simply to brag about their profits. They usually maintain these photographs and/or videos on their person or in their businesses, residences or cars, on computers, or in the residences of friends or relatives. Smartphones, tablets, cellular phones, digital cameras, and other digital devices, often have the capability to take still photos and videos and save them indefinitely on the device's storage medium. Those smuggling contraband frequently use these devices to take their photographs and videos.

17. Documents showing who owns, occupies, or controls the location being searched also show who is responsible for the items found on the premises, including contraband and other evidence seized. Documents and items showing the identity of the persons owning, residing in or controlling the area being searched include, but are not limited to, utility and telephone bills, canceled envelopes and correspondence, outgoing answering machine messages, tax returns, keys, deeds and mortgage receipts. These documents may also be produced on computers, downloaded from online accounts or scanned into digital format and stored on computers and related digital media.

18. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, smartphones, tablets, server computers, and network hardware. The term "digital media" includes personal digital assistants (PDAs), smartphones, tablets, BlackBerry devices, iPhones, iPods, iPads, digital cameras, and cellular telephones. The term "storage media" includes any physical

object upon which electronic data can be recorded, such as hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media or digital medium. Collectively, the terms "computer," "digital media," and "storage media" are referred to as "electronic media."

19. A list of items agents seek authority to seize is in Attachment B.

ELECTRONIC MEDIA AND FORENSIC ANALYSIS

20. As described above and in Attachment B, this application seeks permission to search for evidence and records that might be found on the PREMISES, in whatever form they are found. Much of the evidence and records described in the paragraphs above, and in Attachment B, can also be produced and/or stored on electronic media. For this reason, I submit that if a computer, digital medium, or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer, digital medium, or storage medium. Thus, the warrant applied for would authorize the seizure of electronic media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

21. *Necessity of seizing or copying entire electronic media.* In most cases, a thorough search of a premises for information that might be stored on electronic media often requires the seizure of the physical electronic media and later off-site review consistent with the warrant. In lieu of removing electronic media from the premises, it is sometimes possible to make an image copy of electronic media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the electronic media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

f. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. Electronic media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

g. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the electronic media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

h. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of electronic media formats that may require off-site reviewing with specialized forensic tools.

22. *Necessity of seizing or copying entire electronic media.* In most cases, a thorough search of a premises for information that might be stored on electronic media often requires the seizure of the physical electronic media and later off-site review consistent with the warrant. In

lieu of removing electronic media from the premises, it is sometimes possible to make an image copy of electronic media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the electronic media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying electronic media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the computer or entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

24. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint

scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more

convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped

with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the PREMISES and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the PREMISES and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate

the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

PROBABLE CAUSE

INVESTIGATION BACKGROUND

25. On October 30, 2024, the VGTF along with members of the USMS, and other law enforcement agencies executed 18 search and arrest warrants aimed at disrupting the flow of controlled substances into CCCC (reference Case No. MR 24-1983 through MR 24-1995). I was assigned to a search location in Grants, NM. The results of the October 30 operations resulted in the seizure of firearms, ammo, fentanyl, methamphetamine, approximately $6,000 in cash, cell phones, and 10 arrests.

26. As part of the investigation efforts into the October 30, 2024 operation, VGTF agents reviewed all available information on the inmates, staff, and persons outside the jail involved in smuggling, distributing, and profiting from the illicit trafficking of contraband inside CCCC. VGTF agents reviewed intelligence information, reports, phone calls, letters, writings, and other pertinent information spanning the past three years. VGTF agents also interviewed current and former CCCC inmates about the drug trafficking activities taking place at CCCC.

27. One of the subjects of the current investigation, Estrella Gonzalez, was living at 1812 Del Norte Drive SW, Albuquerque New Mexico (Premises A-1) at the time of these initial search warrants.

28. During the initial search warrant, agents discovered a firearm, at least one thousands dollars in cash, and a suspected drug ledger within Premises A-1. Estrella Gonzalez was not charged with any crimes at that time.

CONTRABAND INTRODUCTION

29. On May 19, 2025, USMS Inmate Adrian Garcia was transported to the Pete V. Domenici United States Courthouse for his criminal trial under Case No. 22-CR-1171.

30. Before Garcia's criminal trial commenced, two Deputy United States Marshals ("DUSMs") were presented with a formal suit, pants, shirt, shoes, and socks for Garcia to wear during his upcoming trial. This clothing was provided by one of Garcia's "family members" outside of the Federal Courthouse around approximately 8:00 AM.

31. At approximately 8:30 AM, the attire was then searched by members of the USMS cellblock during a routine security screen. During a search of this clothing, a DUSM discovered a hidden compartment sewn into the waistband of the pants. Upon closer inspection, the DUSM discovered four orange packages wrapped in cellophane within the compartment. The suspected narcotics were recovered from the pants and seized as evidence.

32. During a field test of the suspected narcotics, DUSMs confirmed that the narcotics were four packages of suboxone strips, measuring approximately 1 inch wide by ¼ inch thick.

33. Based on my training and experience, I believe that Garcia intended to smuggle the suboxone strips from court back into CCCC for resale. The number of strips involved is too large for personal use, and they would not have significant resale value within the federal courthouse proper.

34. Investigators began reviewing Garcia's recorded jail calls to identify others involved in the smuggling attempt.

RECORDED PHONE CALLS

35. On May 17, 2025, Garcia attempted to call (505) 544-1783 from his assigned phone pin[2] at 07:20 PM, but the call recipient did not answer.

36. On May 17, 2025, at 07:22 PM, Garcia placed a second call to (505) 544-1783—this time from USMS Inmate Steven Oneil's account. During the phone call, Garcia referred to the recipient as "Johnny." Garcia told Johnny that he had a trial on Monday, May 19. Garcia stated that he needed help taking "something to his attorney." Garcia added that he was "gonna have someone reach out" to Johnny to bring him the "item."

37. USMS investigators then used CashApp records, including a profile photograph, to identify the "Johnny" using the (505) 544-1783 phone number as Johnny Gutierrez.

38. On May 18, 2024, USMS Inmate Jerry Bezie called (505) 389-5253 at approximately 7:16 PM. USMS Investigators have identified this number through prior and current investigations as used by Estrella Gonzalez. Gonzalez is Jerry Bezie's wife. Agents are familiar with her from several prior investigations, during which they suspect her of assisting Bezie and other drug smugglers attempting to introduce contraband into CCCC.

39. During the phone conversation, Bezie provided Estrella Gonzalez with Johnny Gutierrez's phone number and told her to "drop 'that' off." Based on prior investigations I know that Bezie and Gonzalez spoke in code to avoid making incriminating statements over the recorded phone line.

40. On May 19, 2025, Garcia called Gutierrez again, this time using USMS Inmate Joseph Pedroa-Granados's account. During the call Gutierrez confirmed that he had the clothing.

[2] USMS Inmates at the CCCC are assigned a unique "pin" or number to make phone calls under their account. Inmates involved in contraband smuggling often use other inmates' accounts to avoid scrutiny from law enforcement.

Garcia then directed Gutierrez to drop it off to Garcia's attorney and "tell him that 'he' just bought them." In other words, Garcia ordered Gutierrez to falsely claim that the clothes had just been purchased.

CONCLUSION

41. I believe, based on my training and experience in this investigation, along with the recorded phone call evidence that Garcia, Gutierrez, and Gonzalez all had knowledge of the smuggling attempt.

42. I also know that drugs like suboxone strips are often sold within Cibola, are potentially worth many times their value on the streets of Albuquerque.

43. I further believe, based on my training and experience in this investigation, that additional evidence will likely be stored Gutierrez and Gonzalez's houses, alongside any other contraband that they have been paid to introduce in the future. Messages coordinating this "drop" will almost certainly be contained in their mobile phones. Evidence of the purchase of the suboxone, or other controlled substances, is also likely to be contained in their residences.

44. For these reasons, I believe that evidence of the Target Offenses will be located at the both Subject Premises.

THE SUBJECT PREMISES

45. **Subject Premises A-1**: I believe Estrella Gonzalez, lives at Subject Premises A-1, located at 1812 Del Norte Drive SW, Albuquerque, NM 87105. The Subject Premises may be described as a single-story residence, with light brown stucco siding, white bars over the windows, with a wooden porch. The numbers 1812 are posted on the mailbox in front of the Subject Premises. There are video cameras posted all over the exterior of the property. There is a large

garage and camper located on the property. Color photographs of the Subject Premises have been attached and incorporated in Attachment A-1.

46. Indicia of residence include:

a. According to county records, Gonzalez's associate, Jerry Bezie, owns the Subject Premises.

b. State court documents have listed the Subject Premises as the residence of record for Gonzalez.

c. Open-source records list the Subject Premises as Gonzalez's residence.

d. Within the last two weeks, surveillance agents have observed Gonzalez at the Subject Premises.

47. **Subject Premises A-2**: I believe Johnny Gutierrez lives at Subject Premises A-2, located at 2012 Commercial St SE, Apt A, Albuquerque, NM 87102. The Subject Premises may be described as an apartment style building. Premises A-2 is located on the far left of the apartment complex. It is a tan-colored building with two 6ft tall plants on both sides of the metal screened door. A trash can marked with the letter "A" sits along the alley way to the apartment.

48. Indicia of residence include:

a. MVD records show that Gutierrez has the Subject Premises listed on his current and valid New Mexico Driver's License.

b. State court documents have listed the Subject Premises as the residence of record for Gutierrez.

c. Gutierrez owns a 1996 white Chevrolet Trailblazer that is registered at the Subject Premises. This vehicle has been seen parked outside the property during surveillance.

CONCLUSION

49. I submit that this affidavit supports probable cause for a warrant to search the Subject Premises, further described in Attachments A-1 and A-2, for the things described in Attachment B.

50. This affidavit was reviewed by Assistant United States Attorney David Hirsch.

Respectfully submitted,

Tyler Foster
Deputy United States Marshal

Electronically signed and telephonically sworn on May 20, 2025.

The Hon. Laura Fashing
United States Magistrate Judge
District of New Mexico

ATTACHMENT A-2

Premises to be Searched: The Subject Premises A-2 is located at 2012 Commercial St SE Apt A, Albuquerque, NM 87102. The Subject Premises may be described as an apartment-style building. Premises A-2 is located on the far left of the apartment complex. It is a tan-colored building with two 6ft tall plants on both sides of the metal screened door. A trash can marked with the letter "A" sits along the alley way to the apartment.

The search of the Subject Premises shall include the entire residence and all outbuildings, trash cans, and storage containers designated for use by the occupants of the Subject Premises. The search of the subject premises shall include all persons located on the PREMISES on which the items to be seized could be concealed. The search shall also include vehicles parked at, or in front of, the Subject Premises, provided such vehicle has an apparent connection to the Subject

Premises. Connection to the Subject Premises may be established by way of prior law enforcement observation, vehicle registration, subject admission or possession of an ignition key.

ATTACHMENT B

Property to be seized

All records, information, and evidence relating to violations of:

a. 21 U.S.C. § 846: Conspiracy to Distribute Controlled Substances, and

b. 18 U.S.C. §§ 371 and 1791: Conspiracy to Provide a Prohibited Object to an Inmate of a Prison;

those violations involving Estrella Gonzalez and Johnny Gutierrez and occurring after May 1, 2025, including:

1. Evidence of unexplained income, including large amounts of U.S. Currency and large deposits at banks or mobile payment applications that are inconsistent with income from legitimate sources.
2. Any documents referencing inmates at the Cibola County Correctional Center.
3. Messages, notes, correspondence, and/or communications between Estrella Gonzalez, Johnny Gutierrez, Adrian Garcia, and inmates at the Cibola County Correctional Center.
4. Notes or ledgers containing telephone numbers and potential addresses for co-conspirators.
5. Controlled substances, including, but not limited to, methamphetamine and suboxone.
6. Firearms and ammunition, including handguns, rifles, shotguns and automatic weapons.
7. Telephone toll records for mobile phones owned or controlled by suspected co-conspirators, or other communication devices used by them and/or their drug trafficking associates.
8. Digital video surveillance systems, including the associated storage media.

9. Indications of ownership or control of said premises, including but not limited to, utility bills, cancelled checks, or envelopes and deeds or leases.
10. Indications of ownership or control over any vehicles located at the place to be searched, including but not limited to, titles, registrations, gas receipts, repair bills and keys belonging to that vehicle.
11. Photographs or videos, their co-conspirators and the property and assets purchased with drug proceeds.
12. Any and all computers, digital media, and storage media that reasonably appear to contain some or all of the records, information, and/or evidence described in Attachment B.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer, digital media, or storage media; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "digital media" includes personal digital assistants (PDAs), smartphones, tablets, BlackBerry devices, iPhones, iPods, iPads, digital cameras, and cellular telephones.

The term "storage media" includes any physical object upon which electronic data can be recorded, such as hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media or digital medium.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, smartphones, tablets, server computers, and network hardware.

This warrant authorizes a review of all electronic media seized pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The warrant also authorizes a review of all electronic media for evidence of who used, owned, or controlled the electronic media at the time the things described in this warrant were created, edited, or deleted. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, law enforcement may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the PREMISES described in Attachments A-1 and A-2, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual who is found at the PREMISES and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.